Available online at www.sciencedirect.com

ScienceDirect

Procedia Engineering 128 (2015) 12 – 14

Procedia Engineering

www.elsevier.com/locate/procedia

3rd European STAMP Workshop, STAMP EU 2015

STPA-based method to identify and control feature interactions in large complex systems

John Thomas[a,]*, Dajiang Suo[a]

[a]*Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139-4307, U.S.A.*

Abstract

This research develops and evaluates a new approach that can be applied during STPA Step 1 (identify Unsafe Control Actions) to efficiently identify complex feature interactions among multiple controllers that can result in dysfunctional system behavior. The new approach is applied and evaluated using several automated automotive systems with an emphasis on controllers that may interact or interfere with each other directly or indirectly. The approach is shown to analyze hundreds of interactions with an order of magnitude less effort than has been possible previously. In addition, formal methods are applied to support reasoning about completeness and to enable tool assistance during the search for dysfunctional interactions. Humans are explicitly included as controllers that may interact with automated systems, and accident scenarios involving complex human interactions such as software-induced human errors can be identified.

Peer-review under responsibility of the organizing committee of STAMP EU 2015

Keywords: System safety; STAMP; STPA; hazard analysis; causal factors; feature interactions; multiple controllers

1. Background

Systems-Theoretic Process Analysis (STPA) is a new hazard analysis technique that addresses many growing causes of accidents including requirements flaws, design errors, complex human behavior, and dysfunctional component interactions as well as traditional component failures [1]. Although STPA provides a framework to capture multiple controller interactions, analyzing individual interactions one by one can be labor-intensive. An early informal technique to address feature interaction was presented in 2014 [3], but it was initially applied and evaluated using a

*Corresponding author. Tel: +16174523044
E-mail address: jthomas4@mit.edu

Peer-review under responsibility of the organizing committee of STAMP EU 2015
doi:10.1016/j.proeng.2015.11.499

small system with only 3 software controllers. This research proposes a technique that is scalable to hundreds of controllers and demonstrates the process on real automotive systems with more complexity. In addition, the driver is explicitly included as a controller and dysfunctional human-computer interactions can be quickly and efficiently identified.

2. Case study

In this research, new procedures are developed and applied to several automotive subsystems that must be integrated into a single vehicle platform. The subsystems include a number of automated software controllers, including shift-by-wire, auto-hold, engine stop-start, adaptive cruise control, emergency braking, and push-button ignition. Most automotive manufacturers are now providing or developing similar functionality for their vehicles. These subsystems were chosen to maximize the number of potential interactions that must be controlled. For example, many of these systems directly affect the vehicle propulsion and can easily introduce unsafe interactions such as automatically shifting to park while cruise control is active. The operation of these systems also depends on interactions with the driver, such as enabling/disabling features or correctly responding to various warnings or faults. Therefore, these systems provide ample opportunity to explore unsafe or dysfunctional interactions.

4. Proposed analysis method

The proposed new process begins with the control actions to be analyzed by STPA Step 1. Instead of enumerating all possible combinations of control actions (a very lengthy process), the new process starts by identifying certain properties of the control actions. Once these properties have been defined, a search algorithm can be applied to compare properties of different control actions. Combinations of control actions that may lead to unsafe system behavior can then be identified quickly and efficiently from the search results. It is hypothesized that careful reasoning about individual control action properties can lead to a much more efficient and scalable process than enumerating and analyzing all possible combinations, of which there may be hundreds or thousands in real systems.

In general, two types of properties can be defined: 1) prerequisites or required process conditions and 2) controlled process effects. These properties can be readily identified from context tables if STPA Step 1 is being done formally as in [2], or they can be identified from the context part of Unsafe Control Actions if STPA is being done traditionally as in [1]. Once these properties have been identified, the search algorithm can compare properties from different control actions to identify conflicts that would arise from multiple controllers operating concurrently. Once the conflicts are identified, STPA Step 2 can proceed as usual to identify potential causes of the conflicts and either eliminate the conflict or develop preventative measures.

5. Preliminary results

This research demonstrates the proposed process by applying it in a case study with real automotive control systems and hundreds of potential dysfunctional interactions. It is shown that defining control action properties is a task that grows linearly as more controllers and control actions are added, as opposed to the exponential growth of traditional approaches such as Use Cases.

Although the search portion of the proposed process is not linear, the time required to perform the search does not dominate the overall process and is shown to be insignificant compared to the task of identifying control action properties. While human engineers may be better able to identify control action properties, the search can be performed automatically by tools thereby reducing human workload as well as the potential for mistakes. In the case study example for this research, the overall time required to apply the new process and derive results is found to be an order of magnitude quicker than traditional techniques.

This process is also easily formalized, providing a framework to reason about completeness. In addition, pairwise interactions can be identified just as easily 3-way or N-way interactions, unlike traditional approaches that rely on enumerating all combinations upfront and individually analyzing them. Given these preliminary results, the new technique appears to be much more scalable to complex systems than existing techniques.

References

[1] N.G. Leveson, Engineering A Safer World: Systems Thinking Applied to Safety, MIT Press, Cambridge, MA, 2011
[2] J. Thomas, Extending and Automating A Systems-Theoretic Hazard Analysis For Requirements Generation And Analysis, PhD Thesis, MIT, Boston, 2013.
[3] J. Thomas, S. Placke, Analyzing Feature Interaction in Automobiles, MIT STAMP Workshop, Boston, 2014.